Paso 5. La Seguridad en su red Inalámbrica

Aquí tiene una serie de simples pasos para optimizar la seguridad de su red inalámbrica y proteger sus datos de ojos y oídos entrometidos. Esta sección está orientado para usuarios en el hogar, SOHO (small office & home office).

Importante: Los procedimientos necesarios para completar estos pasos a menudo difieren para cada fabricante. Cuando vea esta imagen , deberá buscar en el manual correspondiente para el correcto procedimiento a seguir.

- Conecte con WEP (Wired Equivalent Privacy)
- Cambie su Password por defecto
- Cierre su Red (si es posible)
- Cambie el nombre de la Red
- Mueva su Access Point
- Use las Tablas de Control MAC
- Otras soluciones elementales
- Use una VPN (Virtual Private Network)
- Información Adicional

- **Conecte con WEP (Wired Equivalent Privacy)**

Lo mas importante: Conecte con WEP (Wired Equivalent Privacy) –Privacidad equivalente a una red cableada-. . WEP está detrás de la tecnología provista por el estándar Wi-Fi (802.11b). Aunque WEP no es perfecto, provee de seguridad básica. Algunos expertos dicen que del 60 al 80% de todas las redes inalámbricas operan sin tener activados el servicio WEP.

La mayoría de las redes Wi-Fi en el hogar y pequeñas oficinas, disponen de encriptación de WEP de 40 bits (también llamada 64 bits). Para efectuar una instalación inicial simple, la mayoría de los access points se entregan con el servicio WEP desconectado. Por lo que una vez que ha implementado su red inalámbrica y está operativa, esté seguro de que activa WEP siguiendo las siguientes instrucciones del manual de instrucciones del fabricante.

También se puede incrementar su seguridad cambiando periódicamente la clave de encriptación. Si está preocupado sobre la seguridad de su red inalámbrica, cambie su clave cada semana, o como máximo cada dos. Si su preocupación es mayor, cambien la clave mas a menudo o utilice tecnología avanzada de seguridad como 802.1x que le permite cambiar el código WEP automáticamente cada 5 minutos.

Vea en la Sección 4 Configuraciones Wi-Fi. Conectarse en movilidad.

Caverin Solutions S.A.
C/ Aribau, 103 entlo. 1
08036 Barcelona
Tlfno: 933239342

La mayoría de las redes inalámbricas se entregan al cliente con una Password por defecto que provee el fabricante. Cámbiela lo antes posible.

- **Cierre su Red (si es posible)**

Si es posible, bloquee el SSID (Service Set Identifier) para que no pueda ser difundido . Esto tiene el efecto de “cerrar” la red. Muchos sistemas Wi-Fi te permiten ejecutar esta función.

Todos los APs se entregan con una señal inalámbrica guía por lo que los PCs inalámbricos pueden de manera mas sencilla encontrarlos. En efecto, esta señal está “gritando”, “Estoy aquí”, Conéctate!. Desconectando el servicio SSID o cerrando su red, hará que esta sea mas fuerte y más difícil que los hackers la intercepten. Si los hackers no saben de la existencia de tu red, tienen menos oportunidades de utilizar tu tiempo en “crackear” las comunicaciones de su empresa. Por lo que si su equipamiento lo permite, cierre la red y comprueba de que lo ha efectuado

- **Cambie el nombre de la Red**

La mayoría de los APs se entregan con un nombre de red por defecto. Cuando su red está operativa y funcionando, debería de cambiarle el nombre por algo mas personal, difícil de adivinar. En otras palabras, si su apellido es Vázquez, no le llame Vázquez a su red. Muchas compañías, incluso grandes corporaciones, nombran a sus redes con el nombre de la Compañía o sus direcciones. No lo haga, Sea creativo. Se recomienda una combinación de letras y números y no utiliza la calle de su dirección!

- **Mueva su Access Point**

Para aumentar la privacidad, coloque los APs en medio de la sala, evite ventanas abiertas y puertas. Contra mas madera y metal halla en el entorno, menor será la distancia que sus mensajes inalámbricos podrán alcanzar. Puede testar que cantidad de señal se escapa de su negocio o de su vivienda cogiendo su portátil equipado con Wi-Fi y saliendo fuera de la sala a la calle y chequear hasta donde se puede alejar y seguir manteniendo la conexión. Se sorprenderá.

- **Use las Tablas de Control MAC**

Use las tablas MAC (Medium Access Control) si sus APs las soporta. . Como todo los periféricos de red, los dispositivos de radio Wi-Fi disponen de una dirección única MAC codificada en la memoria interna.. Usando el MAC Access Control List (ACL), podrá limitar las conexiones inalámbricas solo a los dispositivos de radio Wi-Fi cuyas direcciones MAC están directamente

Caverin Solutions S.A.
C/ Aribau, 103 entlo. 1
08036 Barcelona
Tlfno: 933239342

conectadas a su AP. Es un proceso similar al de bloquear ciertas llamadas en un teléfono, pero en una red inalámbrica. Si un intruso con un dispositivo de radio inalámbrico con una dirección MAC que no aparece en esta tabla, se intenta conectar a su red, su AP no se lo permitirá.

- **Otras soluciones elementales**

Existen diversas formas de definir los directorios de sus ordenadores y redes para proteger sus ficheros almacenados y los datos. Una forma es desconectar la función “Sharing” y usar “Passwords” para acceder a los directorios que tengan ficheros confidenciales. Los servicios de Sharing and Passwords se acceden desde Windows cliqueando con el botón derecho del ratón en el directorio en cuestión y yendo a “Propiedades”. Vea también Windows Tips.

Recuerde que la mayoría de los sitios web que gestionan compras on line, tarjetas de crédito y cualquier tipo de información financiera, normalmente usan métodos de encriptación como SSL (secure socked layer) para proteger datos confidenciales. Así, la mayoría de los datos financieros que se transmiten en Internet están ya codificados desde el momento que salen de su PC hasta que llega al sitio web.

- **Use una VPN (Virtual Private Network)**

La mayoría de las grandes Compañías usa tecnologías VPN (Virtual Private Network) para el personal que necesita acceso remoto a las bases de datos corporativas de las Compañías. El sistema VPN también trabaja con redes locales inalámbricas.

Una VPN crea un túnel virtual desde su ordenador a través del AP inalámbrico, hacia Internet, y desde ahí hacia la sede central de su compañía. Aunque parezca complicado y caro, usar VPN crea casi siempre un muro impenetrable de seguridad para sus comunicaciones inalámbricas aunque esté trabajando desde los lugares mas variados: desde su casa, la sala de espera de un aeropuerto o la sala de juntas de su empresa.

Caverin Solutions S.A.
C/ Aribau, 103 entlo. 1
08036 Barcelona
Tlfno: 933239342